

併合親 2002-332404

US

924

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 2 年 1 1 月 1 9 日

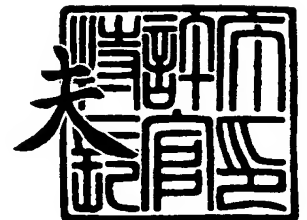
出 願 番 号
Application Number: 特 願 2 0 0 2 - 3 3 5 4 0 1
[ST. 10/C]: [J P 2 0 0 2 - 3 3 5 4 0 1]

出 願 人
Applicant(s): 日本電気株式会社
日本電気通信システム株式会社

2 0 0 3 年 9 月 2 5 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 0 7 8 9 5 6

【書類名】 特許願

【整理番号】 49200232

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/06
H04L 9/14

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 地引 昌弘

【発明者】

【住所又は居所】 東京都港区芝五丁目 7 番 1 号 日本電気株式会社内

【氏名】 鈴木 一哉

【発明者】

【住所又は居所】 東京都港区三田一丁目 4 番 2 8 号 日本電気通信システム株式会社内

【氏名】 馬越 英之

【特許出願人】

【識別番号】 000004237

【氏名又は名称】 日本電気株式会社

【特許出願人】

【識別番号】 000232254

【氏名又は名称】 日本電気通信システム株式会社

【代理人】

【識別番号】 100093595

【弁理士】

【氏名又は名称】 松本 正夫

【手数料の表示】

【予納台帳番号】 057794

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9303563

【包括委任状番号】 0100121

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ストリームメディアデータのスクランブル放送システム

【特許請求の範囲】

【請求項 1】 配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて、

前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、

前記配信側は、所定の時間的間隔で、前記鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、

前記受信側は、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行うことを特徴とするストリームメディアデータのスクランブル放送システム。

【請求項 2】 ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更することを特徴とする請求項 1 に記載のストリームメディアデータのスクランブル放送システム。

【請求項 3】 入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行うことを特徴とする請求項 1 又は請求項 2 に記載のストリームメディアデータのスクランブル放送システム。

【請求項 4】 前記ストリームメディアデータの種類に応じて、前記鍵ビットパターンのビット数を増減することを特徴とする請求項 1 から請求項 3 の何れか 1 項に記載のストリームメディアデータのスクランブル放送システム。

【請求項 5】 前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの 2 つのビ

ットパターンを用いて、前記符号化と復号化を行うことを特徴とする請求項 1 から請求項 4 の何れか 1 項に記載のストリームメディアデータのスクランブル放送システム。

【請求項 6】 前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込むと共に、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得することを特徴とする請求項 1 から請求項 5 の何れか 1 項に記載のストリームメディアデータのスクランブル放送システム。

【請求項 7】 配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて前記ストリームメディアデータの符号化と復号化を実行するスクランブル処理プログラムであって、

前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、

前記配信側で、所定の時間的間隔で、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行し、

前記受信側で、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行することを特徴とするスクランブル処理プログラム。

【請求項 8】 ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更する機能を有することを特徴とする請求項 7 に記載のスクランブル処理プログラム。

【請求項 9】 入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行う

機能を有することを特徴とする請求項 7 又は請求項 8 に記載のスクランブル処理プログラム。

【請求項 1 0】 前記ストリームメディアデータの種類のに応じて、前記鍵ビットパターンビット数のビット数を増減する機能を有することを特徴とする請求項 7 から請求項 9 の何れか 1 項に記載のスクランブル処理プログラム。

【請求項 1 1】 前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの 2 つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする請求項 7 から請求項 1 0 の何れか 1 項に記載のスクランブル処理プログラム。

【請求項 1 2】 前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込む機能を有し、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得する機能を有することを特徴とする請求項 7 から請求項 1 1 の何れか 1 項に記載のスクランブル処理プログラム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ストリームメディアデータのスクランブル放送システムに関し、特に専用ハードウェアなどを特に必要とせず簡単に符号化と復号化を行うことを可能とするストリームメディアデータのスクランブル放送システムに関する。

【 0 0 0 2 】

【従来の技術】

インターネットを利用したストリームメディアデータの配信放送、衛星放送、ケーブルテレビ放送などの、ストリームメディアデータの放送については、ビジネス上の理由から、コンテンツの保護を行なうスクランブル放送が要求されている。従来、このストリームメディアデータのスクランブルとしては、主に DES や AES、RSA などの暗号化アルゴリズムが用いられてきている。

【 0 0 0 3 】

これらのアルゴリズムは、強力な暗号化が可能である一方、ソフトウェアで符号化／復号化を行なうには多くの処理が必要であり、特に放送データのようなリアルタイムの符号化／復号化を行なう場合には、専用のハードウェアが必要である。放送サービス用のスクランブル装置は、各家庭に広く普及させる必要があるものの、このようなコスト面における問題は普及の障壁となっている。

【 0 0 0 4 】

ストリームメディアデータのスクランブル放送方式に関する従来技術としては、例えば、特開平 8 - 2 8 8 9 3 9 号公報に開示されている技術等が提案されている。この特開平 8 - 2 8 8 9 3 9 号公報においては、回線終端装置の暗号鍵発生部によって生成される暗号鍵によって放送セルを暗号化すると共に、加入者端末が予め付与された暗号鍵を用いて放送セルを復号化する方法が開示されている。

【 0 0 0 5 】

【発明が解決しようとする課題】

上述したように、従来のストリームメディアデータのスクランブル放送方式では、特殊な暗号化アルゴリズムを用いるためストリームメディアデータのスクランブルのために専用のハードウェアを備える必要があるため、ストリームメディアデータの配信及び受信を行うためにコストがかかり、普及を妨げる要因となっていた。

【 0 0 0 6 】

例えば、上述した特開平 8 - 2 8 8 9 3 9 号公報の技術でも、暗号鍵によって放送セルを暗号化するための、及び暗号化された放送セルを復号するための専用のハードウェア装置が必要となる。

【 0 0 0 7 】

本発明の目的は、ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を符号化及び復号化のための専用ハードウェアなどを特に必要とせず簡単に行なうことを可能にするストリームメディアデータのスクランブル放送方式を提供することにある。

【 0 0 0 8 】

本発明の他の目的は、ソフトウェアによる処理でも高速な符号化及び復号化を行なうことができるストリームメディアデータのスクランブル放送方式を提供することにある。

【0 0 0 9】

本発明のさらに他の目的は、ストリームメディアデータのスクランブルにおける鍵の強度を実用的なレベルまで上げることができるストリームメディアデータのスクランブル放送方式を提供することにある。

【0 0 1 0】

【課題を解決するための手段】

上記目的を達成する本発明は、配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置を備え、前記配信側は、所定の時間的間隔で、前記鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、前記受信側は、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行うことを特徴とする。

【0 0 1 1】

請求項 2 の本発明のスクランブル放送システムは、ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前記鍵ビットパターンを変更することを特徴とする。

【0 0 1 2】

請求項 3 の本発明のスクランブル放送システムは、入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行うことを特徴とする。

【0 0 1 3】

請求項 4 の本発明のスクランブル放送システムは、前記ストリームメディアデ

ータの種類に応じて、前記鍵ビットパターンビット数を増減することを特徴とする。

【0014】

請求項5の本発明のスクランブル放送システムは、前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの2つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする。

【0015】

請求項6の本発明のスクランブル放送システムは、前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込むと共に、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得することを特徴とする。

【0016】

請求項7の本発明は、配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムにおいて前記ストリームメディアデータの符号化と復号化を実行するスクランブル処理プログラムであって、前記配信側で、所定の時間的間隔で、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置から生成される異なる前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行し、前記受信側で、前記配信側と同じ前記鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う機能を実行することを特徴とする。

【0017】

請求項8の本発明のスクランブル処理プログラムは、ストリームメディアデータの一定のデータ量毎に、前記鍵ビットパターンを変更することにより、前記配信側と前記受信側が、前記一定のデータ量に基づいて符号化と復号化に使用する前

記鍵ビットパターンを変更する機能を有することを特徴とする。

【 0 0 1 8 】

請求項 9 の本発明のスクランブル処理プログラムは、入力されたストリームメディアデータに対して、前記鍵ビットパターンを用いて排他的論理和をとることにより、前記符号化と復号化を行う機能を有することを特徴とする。

【 0 0 1 9 】

請求項 1 0 の本発明のスクランブル処理プログラムは、前記ストリームメディアデータの種類のに応じて、前記鍵ビットパターンのビット数を増減する機能を有することを特徴とする。

【 0 0 2 0 】

請求項 1 1 の本発明のスクランブル処理プログラムは、前記鍵ビットパターン生成装置によって生成された前記鍵ビットパターンと、当該鍵ビットパターンを反転させたビットパターンの 2 つのビットパターンを用いて、前記符号化と復号化を行うことを特徴とする。

【 0 0 2 1 】

請求項 1 2 の本発明のスクランブル処理プログラムは、前記ストリームメディアデータを符号化する際に、前記鍵ビットパターンを一意に識別する情報を、ストリームメディアデータに埋め込む機能を有し、前記ストリームメディアデータの復号化の際に、前記埋め込まれた前記鍵ビットパターンの情報によって復号化に用いる前記鍵ビットパターンを前記鍵ビットパターン生成装置から取得する機能を有することを特徴とする。

【 0 0 2 2 】

【発明の実施の形態】

以下、本発明の好ましい実施の形態について図面を参照して詳細に説明する。

【 0 0 2 3 】

図 1 は、本発明によるストリームメディアデータのスクランブル放送方式を適用した実施の形態のシステム構成を示すブロック図である。

【 0 0 2 4 】

この実施の形態によるシステムは、ストリームメディアデータの符号化（スク

ランブル) ”を行なうスクランブル装置 1 0 と、符号化されたストリームメディアデータの復号化（スクランブルの解除）を行なうスクランブル解除装置 2 0、及び符号化／復号化処理において排他的論理和を取るための鍵ビットパターンを生成する鍵ビットパターン生成装置 3 0 を含む。

【 0 0 2 5 】

スクランブル装置 1 0 は、図 2 に示す一例のように、インターネット等の通信回線上でコンテンツであるストリームメディアデータの配信サービスを行うサービス業者（サービスプロバイダ等）のサーバ 1 0 0 等にその機能として又はオプションとして備えられる装置であり、入力された生ストリームメディアデータに対し、鍵ビットパターン生成装置 3 0 から配布されて鍵ビットパターン管理部 1 1 が管理する所定の鍵ビットパターンを用いて、ストリーム符号化部 1 2 において排他的論理和による符号化処理を行う。

【 0 0 2 6 】

また、符号化されたストリームメディアデータには、符号化に利用した鍵ビットパターンを一意に識別する識別情報が埋め込まれる。この識別情報により、スクランブル解除装置 2 0 においてストリームメディアデータの復号化を行う際に、必要な鍵ビットパターンを鍵ビットパターン生成装置 3 0 に要求することができる。

【 0 0 2 7 】

なお、スクランブル装置 1 0 は、上記のようにインターネット等の通信回線上でコンテンツであるストリームメディアデータの配信サービスを行うサービス業者に限らず、衛星放送やケーブルテレビ放送を行うサービス業者のストリームメディアデータの配信装置にも、その機能として又はオプションとして備えられる。

【 0 0 2 8 】

符号化されたストリームメディアデータは、ストリーム符号化部 1 2 から出力され、インターネット等のネットワーク上をパケット通信等により配信されてスクランブル解除装置 2 0 へ入力される。

【 0 0 2 9 】

このスクランブル解除装置 2 0 は、図 2 に示す一例のようにコンテンツである

ストリームメディアデータの配信を受ける（放送を受信する）ユーザのクライアント端末（受信装置）200に、その機能として又はオプション（例えば、クライアント端末とモデムとの間に介在）として備えられる装置であり、入力された符号化ストリームメディアデータに対し、鍵ビットパターン生成装置30から配布されて鍵ビットパターン管理部21が管理する所定の鍵ビットパターンを用いて、ストリーム復号化部22において排他的論理和による復号化処理を行う。復号化されたストリームメディアデータは、ストリーム復号化部22から出力され、ユーザのクライアント端末200へ提供され、画像表示装置上に表示される。

【0030】

なお、ケーブルテレビ放送を受信するユーザであれば、上記スクランブル解除装置20は、例えばケーブルテレビのセットトップボックスの機能又はオプションとして備えられる。

【0031】

鍵ビットパターン生成装置30は、インターネット等の通信回線を介して上記放送サービス業者のサーバ100等の装置及びユーザのクライアント端末200等の装置と接続され、それぞれに対してストリームメディアデータの排他的論理和による符号化と復号化に利用する所定の鍵ビットパターンを生成して配布する。

【0032】

この鍵ビットパターン生成装置30は、図2に示す一例のように、サービス業者及びユーザに対して所定の鍵ビットパターンの配布を行う独立した鍵ビットパターン配布サービス業者のサーバ300に、その機能として又はオプションとして備えられている。

【0033】

鍵ビットパターン管理部11及び鍵ビットパターン管理部21は、定期的あるいは所定のデータ量ごとに鍵ビットパターン生成装置30に対して鍵ビットパターンの配布を要求する。

【0034】

また、鍵ビットパターン配布サービス業者のサーバ300では、ストリームメデ

ィアデータを受信するユーザ毎に、鍵ビットパターンの配布量（配布数）を計数して管理することにより、その計数値に応じてユーザからコンテンツの課金（視聴料）を徴収し、放送サービス業者に対して支払うといったサービスを行うこともできる。

【0035】

このようにストリームメディアデータの復号化に必要な鍵ビットパターンの配布量に応じて課金を徴収することにより、確実に配信を受けたストリームメディアデータ量に応じた適切な課金を行うことができると共に、放送サービス業者にとっても課金徴収に伴う負担を軽減することができる。

【0036】

次いで、上記のように構成される本システムの動作について図1～図6を参照して詳細に説明する。

【0037】

まず、生ストリームメディアデータに対して符号化処理（スクランブル処理）を行う動作について説明する。

【0038】

図1のスクランブル装置10に対して入力された生ストリームメディアデータは、鍵ビットパターン管理部11が管理する所定の鍵ビットパターンを用いて、ストリーム符号化部12において符号化されるが、図3及び図4と、図7のフローチャートを参照してその詳細なアルゴリズムを説明する。

【0039】

図3、図4に示す生ストリームメディアデータ40は、スクランブル装置10に入力された符号化される前のストリームメディアデータである。鍵ビットパターン50は、鍵ビットパターン生成装置30が生成し、鍵ビットパターン管理部11を経由して渡される生ストリームメディアデータ40との排他的論理和をとるための鍵ビットパターンである。鍵ビットパターン50のビット数は任意であるが、図3から図6の符号化処理及び復号化処理では4ビットである場合を例として説明する。

【0040】

この鍵ビットパターンとしては、実際の運用においては、例えば 3 2 ビット、1 2 8 ビット、5 1 2 ビット等のビット数が利用される。符号化したストリームメディアデータの機密性は、鍵ビットパターンの鍵として強度に比例して大きくなるので、機密性を大きくしたい場合には鍵ビットパターンのビット数を増やし容易に解除できないようにする。ただし、鍵ビットパターンのビット数を必要以上に大きくしても機密性の大きさは余り変わらず、処理だけに時間がかかってしまうことになる。

【 0 0 4 1 】

ストリームメディアデータの種類（映画やニュース等）に応じて、すなわち機密性に応じて、鍵ビットパターンのビット数を変更するようにすることもできる。

【 0 0 4 2 】

スクランブル装置 1 0 は、生ストリームメディアデータ 4 0 の入力を受け付けると（図 7、ステップ 1 0 1）、この生ストリームメディアデータ 4 0 のスクランブル処理を行う鍵となる鍵ビットパターン 5 0 が鍵ビットパターン管理部 1 1 に存在するかどうかを確認する（ステップ 1 0 2）。すなわち、現在使用している鍵ビットパターン 5 0 が鍵ビットパターン管理部 1 1 に存在するかを確認する。鍵ビットパターン管理部 1 1 では、現在符号化に使用している鍵ビットパターンを、鍵ビットパターンが変更されるまで保持している。

【 0 0 4 3 】

もし、鍵ビットパターン 5 0 が存在しない場合は、鍵ビットパターン生成装置 3 0 に対して要求を出して鍵ビットパターンを受け取る（ステップ 1 0 3）。鍵ビットパターン 5 0 を保持している場合は、以下の手順で符号化処理を実行する（ステップ 1 0 4 からステップ 1 0 8）。

【 0 0 4 4 】

まず、生ストリームメディアデータ 4 0 の先頭から 4 ビット（ビット番号 1 ～ ビット番号 4 の「1 0 0 1」）のデータと鍵ビットパターン 5 0 との排他的論理和をとる（ステップ 1 0 5）。

【 0 0 4 5 】

全ての生ストリームメディアデータ 4 0 についてスクランブルを行ったかを判定しながら（ステップ 1 0 6）、生成されたビット列「0 1 0 0」を、スクランブルストリームデータ 6 1 として保存する（ステップ 1 0 7）。

【0 0 4 6】

続いて、生ストリームメディアデータ 4 0 における次の 4 ビット（ビット番号 5 ～ビット番号 8 の「1 0 1 0」）のデータと鍵ビットパターン 5 0 との排他的論理和をとる。生成されたビット列「0 1 1 1」は、保存されているスクランブルストリームデータ 6 1 の続きに連結される。この手順を繰り返し、生ストリームメディアデータ 4 0 における全てのビットに対して鍵ビットパターン 5 0 による排他的論理和をとる処理を終了した後、最終的に生成され保存されているスクランブルストリームデータ 6 1 を出力する（ステップ 1 0 8）。スクランブルストリームデータ 6 1 は、パケット通信等により通信回線を介してユーザのクライアント端末 2 0 0 に送られ、スクランブル解除装置 2 0 に入力される。

【0 0 4 7】

なお、上記符号化処理に際して、ストリームメディアデータの所定のデータ量単位ごとに、例えば M P E G データであれば、所定パケット数毎に、又は所定の時間間隔ごとに、鍵ビットパターン生成装置 3 0 に要求することにより、使用する鍵ビットパターンを変更する。

【0 0 4 8】

また、鍵ビットパターンを変更するたびに、符号化処理に用いた鍵ビットパターンを一意に識別するための識別情報を埋め込む。パケットであれば、そのヘッダ部分に埋め込む。

【0 0 4 9】

次に、スクランブル解除装置 2 0 において、スクランブルされたストリームメディアデータからスクランブルを外し、生ストリームメディアデータを取り出す動作について図 5 及び図 6、図 8 のフローチャートを参照して説明する。

【0 0 5 0】

図 1 のスクランブル解除装置 2 0 に対して入力されるスクランブルされたストリームメディアデータ（スクランブル装置 1 0 の出力であるスクランブルストリ

ームデータ 61) は、鍵ビットパターン管理部 21 が管理する鍵ビットパターンを用いて、ストリーム復号化部 22 において復号化されるが、図 5、図 6 を参照してその詳細なアルゴリズムを説明する。

【0051】

図 5、図 6 のスクランブルストリームデータ 61 は、鍵ビットパターン管理部 21 に入力された符号化処理された（スクランブルされた）ストリームメディアデータである。

【0052】

スクランブルストリームデータ 61 を復号化する（スクランブルを解除する）鍵ビットパターン 80 は、鍵ビットパターン生成装置 30 が生成し、鍵ビットパターン管理部 21 を経由して渡されるスクランブルストリームデータ 61 との排他的論理和をとるための鍵ビットパターンである。この鍵ビットパターン 80 は、スクランブル装置 10 で生ストリームメディアデータ 40 に対して排他的論理和をとり、スクランブルストリームデータ 61 を生成するに利用した鍵ビットパターン 50 と同じビットパターンを有する。

【0053】

スクランブル解除装置 20 は、スクランブルストリームデータ 61 の入力を受け付けると（図 8、ステップ 201）、このスクランブルストリームデータ 61 のスクランブルを解除する鍵となる鍵ビットパターンが鍵ビットパターン管理部 21 に存在するかどうかを確認する（ステップ 202）。もし、鍵ビットパターンが存在しない場合は、スクランブルストリームデータ 61 に埋め込まれている鍵ビットパターンの識別情報に基づいて鍵ビットパターン生成装置 30 に当該鍵ビットパターンの配布を要求して受け取る（ステップ 203）。すなわち、現在使用している鍵ビットパターン 80 が鍵ビットパターン管理部 21 に存在するかを確認する。ビットパターン管理部 21 では、現在復号化に使用している鍵ビットパターンを、鍵ビットパターンが変更されるまで保持している。

【0054】

鍵ビットパターン 80 を保持している場合又は鍵ビットパターン 80 を取得した場合、以下の手順で復号化処理を行う（スクランブルを解除する）（ステップ

204からステップ208)。

【0055】

まず、スクランブルストリームデータ61の先頭から4ビット（ビット番号1～ビット番号4の「0100」）のデータと鍵ビットパターン80との排他的論理和をとる（ステップ205）。

【0056】

全てのスクランブルストリームデータ61についてのスクランブル解除が終了するまで（ステップ206）、生成されたビット列「1001」は、生ストリームメディアデータ91として保存する（ステップ207）。

【0057】

続いて、スクランブルストリームデータ61における次の4ビット（ビット番号5～ビット番号8の「0111」）のデータと鍵ビットパターン80との排他的論理和をとる。生成されたビット列「1010」は、保存されている生ストリームメディアデータ91の続きに連結して保存される。この手順を繰り返し、スクランブルストリームデータ61における全てのビットに対して鍵ビットパターン80との排他的論理和をとる処理を終了した後、最終的に生成され保存されている生ストリームメディアデータ91を生ストリームメディアデータとして出力する（ステップ208）。

【0058】

スクランブル装置10とスクランブル解除装置20の間では、ストリームメディアデータの所定単位データ量毎に鍵ビットパターンを変更することを予め取り決めておくことにより、スクランブル装置10では所定単位データ量毎に、或いは所定の時間間隔毎に、新たな鍵ビットパターンを鍵ビットパターン生成装置30から取得して符号化処理を行う共に、スクランブル解除装置20では所定単位データ量毎に、スクランブルストリームデータに埋め込まれている識別情報によって新たな鍵ビットパターンを鍵ビットパターン生成装置30から取得して復号化処理を行うようにすれば、符号化と復号化の同期を取ることができる。

【0059】

次に、本発明の他の実施の形態について図面を参照して詳細に説明する。

【0060】

図3から図6の例では、あるストリームメディアデータのある一定量について、1種類の鍵ビットパターンを用いて符号化処理と復号化処理を行なっている。

【0061】

しかし、複数の鍵ビットパターン生成装置20から取得した複数の鍵ビットパターンを同時に用いる、あるいは異なるタイミングで取得した複数の鍵ビットパターンを同時に用いる、あるいは1種類の鍵ビットパターンを反転させて生成した複数の鍵ビットパターンを同時に用いる、あるいはこれらの方法を組み合わせることで、複数の鍵ビットパターンを用いた符号化処理と復号化処理を行なうことも可能である。

【0062】

上記のような方法を用いることにより、1種類の鍵ビットパターンを用いる場合に比べてスクランブルの強度（機密性）を上げることができる。これにより、より多くの種類のストリームメディアデータに対して本発明を適用することができるようになる。

【0063】

図9は、2つの鍵ビットパターンを用いてスクランブル化を行う例を示している。この例では、鍵ビットパターン55は、鍵ビットパターン50を反転させることにより生成している。この鍵ビットパターンの反転は、スクランブル装置10及びスクランブル解除装置20において行われる。これにより、スクランブル装置10及びスクランブル解除装置20では、1つの鍵ビットパターンを共有するだけで、事実上、2つの鍵ビットパターンによる符号化処理及び復号化処理を施すことができる。

【0064】

図9では、入力された生ストリームメディアデータ40に対して、鍵ビットパターン50及び55により排他的論理和をとって符号化することにより、スクランブルストリームデータ303を生成している。生ストリームメディアデータ300のビット番号9以降のデータに対しても、鍵ビットパターン50及び55をその順で適用して排他的論理和をとり、最終的にネットワーク上を配信可能なス

クランブルメディアデータ 303 を生成する。

【0065】

図10は、2つの鍵ビットパターン90と95を用いてスクランブルを解除する例を示している。鍵ビットパターン90及び95は、それぞれ図9においてスクランブルを施す際に用いた鍵ビットパターン50、55と同じ鍵ビットパターンである。スクランブルストリームデータ303に対して、鍵ビットパターン90及び95により排他的論理和をとって復号化することにより、生ストリームメディアデータ401を生成している。スクランブルストリームデータ303のビット番号9以降のデータに対しても、鍵ビットパターン90及び95をその順で適用して排他的論理和をとり、生ストリームメディアデータ401を再生成する。

【0066】

本発明のストリームメディアデータのスクランブル放送方式は、構成要素である各装置の機能をハードウェア的に実現することは勿論として、上記した各装置の機能を実行してストリームメディアデータのスクランブルとスクランブルの解除を行うスクランブル処理プログラム（アプリケーション）を放送サービス業者のサーバ及びユーザのクライアント端末のコンピュータ処理部（CPU）のメモリにロードして実行することで実現することができる。すなわち、スクランブル処理装置及びスクランブル解除装置の機能をソフトウェアによって実現することができる。このスクランブル処理プログラムは、磁気ディスク、半導体メモリその他の記録媒体に格納され、その記録媒体からコンピュータ処理部にロードされ、コンピュータ処理部の動作を制御することにより、上述した各機能を実現する。

【0067】

以上好ましい実施の形態及び実施例をあげて本発明を説明したが、本発明は必ずしも上記実施の形態及び実施例に限定されるものではなく、その技術的思想の範囲内において様々に変形して実施することができる。

【0068】

なお、上記実施の形態においては、ストリームデータに埋め込まれた鍵ビットパ

ターンの識別情報に基づいて、スクランブル解除装置が、鍵ビットパターン生成装置に対して鍵ビットパターンの生成を要求する場合を示したが、ストリームデータに鍵ビットパターンの識別情報を埋め込まず、スクランブル解除装置がスクランブル装置に鍵ビットパターンの識別情報を問い合わせるようにすることも可能である。

【 0 0 6 9 】

【発明の効果】

以上説明したように本発明のストリームメディアデータのスクランブル放送方式によれば、以下に述べるような優れた効果が得られる。

【 0 0 7 0 】

ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を簡潔に行なえるようになる。また、符号化及び復号化のための専用ハードウェアなどを特に必要とせず、携帯端末や家庭内のホームゲートウェイといった小規模な装置でも、符号化及び復号化を用いたストリームメディアデータの放送と受信を容易に行なうことができる。そのため、スクランブル装置及びスクランブル解除装置のコストを従来より引き下げることが可能となり、一般に広く普及させることができる。これにより、パケット通信を用いた放送サービスを本格的に立ち上げることが可能になる。

【 0 0 7 1 】

その理由は、本発明で符号化及び復号化のために利用している鍵ビットパターンによる排他的論理和の処理は、多くのCPUにおいて機械語レベルの命令として実装されているため、ソフトウェアによる処理でも高速に行なえるからである。

【 0 0 7 2 】

なお、スクランブルにおける鍵の強度は、以下の理由により、鍵ビットパターンの有効時間を制限して適宜パターンを変更することにより、実用的なレベルまで上げることができる。

【 0 0 7 3 】

第1に、文字データなどに比べ、ストリームメディアデータでは元の（生の）

データを類推することが困難なため、鍵空間の先頭から鍵を単純に当てはめて解読に成功したかどうかを調べる手法（DESの暗号解読に用いられた手法）や、符号化されたデータを多数収集した後にその傾向を調べるといった手法（一般的暗号解読手法）では解読しにくいこと。すなわち、鍵ビットパターンによる排他的論理和処理を利用した符号化及び復号化によって実用的な鍵の強度を持たせることができる。

【0074】

第2に、ストリームメディアデータ自身が時間と関連した価値を有する場合（例えばニュースの配信など）では、配信から時間を経たデータは情報としての価値が落ちるため、解読に時間をかけることができない。よって、ニュース等のストリームメディアデータの場合には、鍵ビットパターンのビット数が少なくても実用的な鍵の強度を持たせることができる。

【0075】

第3に、排他的論理和の処理は簡単に行なえるため、鍵（ビットパターン）のサイズを必要十分な強度まで増やしても、符号化及び復号化の処理にはあまり影響を与えない。よって、鍵ビットパターンのビット数を増やすことで十分な鍵の強度を与えることができる。

【図面の簡単な説明】

【図1】 本発明の第1の実施の形態によるストリームメディアデータのスクランブル放送システムの構成を示すブロック図である。

【図2】 本発明の第1の実施の形態によるストリームメディアデータのスクランブル放送システムの全体構成示す図である。

【図3】 本発明の鍵ビットパターンを用いて符号化する際のアルゴリズムを説明する図である。

【図4】 本発明の鍵ビットパターンを用いて符号化する際のアルゴリズムを説明する図である。

【図5】 本発明の鍵ビットパターンを用いて復号化する際のアルゴリズムを説明する図である。

【図6】 本発明の鍵ビットパターンを用いて復号化する際のアルゴリズム

を説明する図である。

【図 7】 鍵ビットパターンを用いて符号化するスクランブル装置の動作を説明するフローチャートである。

【図 8】 鍵ビットパターンを用いて復号化するスクランブル解除装置の動作を説明するフローチャートである。

【図 9】 2つの鍵ビットパターンを用いて符号化を行う際のアルゴリズムを説明する図である。

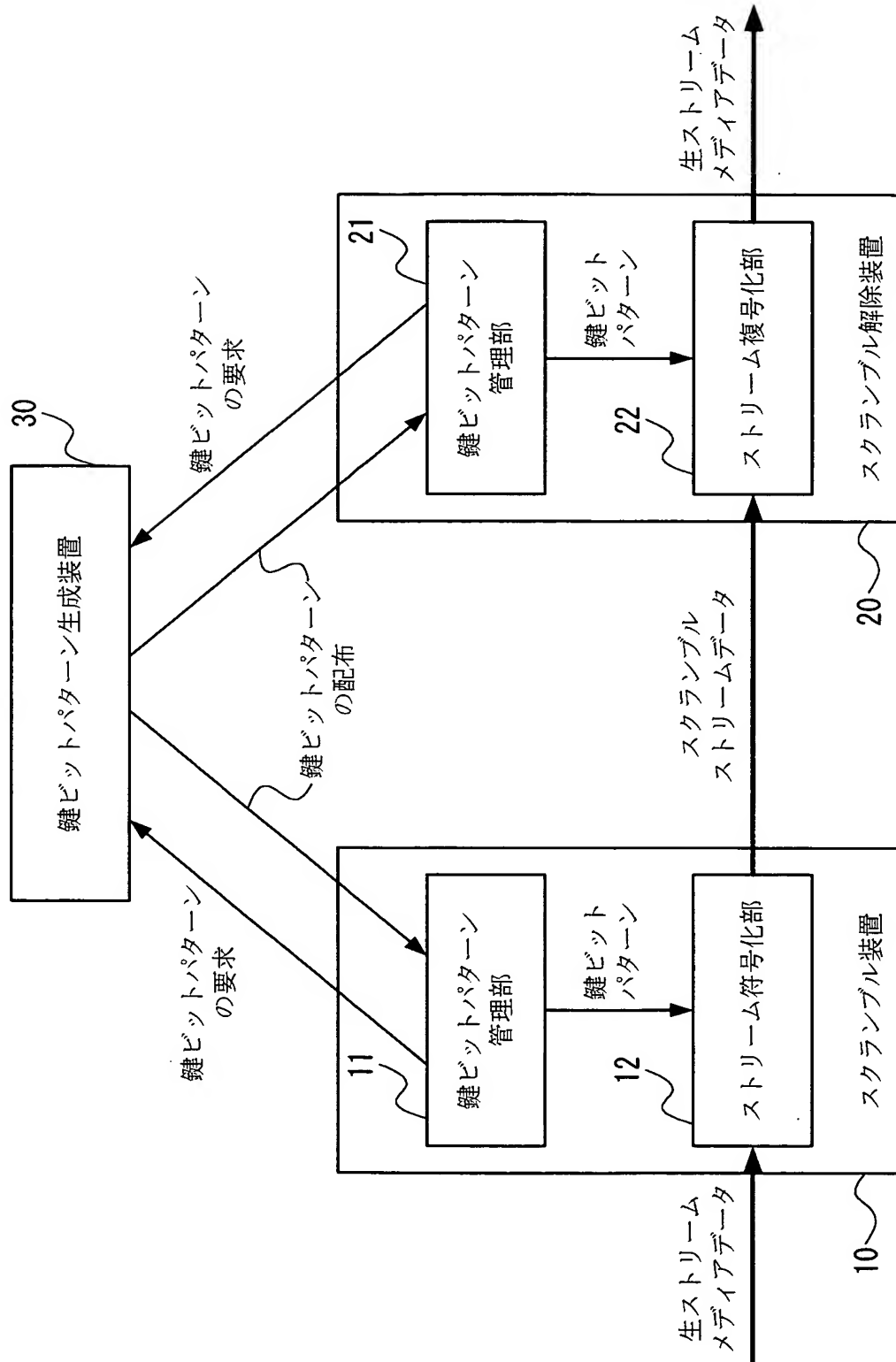
【図 10】 2つの鍵ビットパターンを用いて復号化を行う際のアルゴリズムを説明する図である。

【符号の説明】

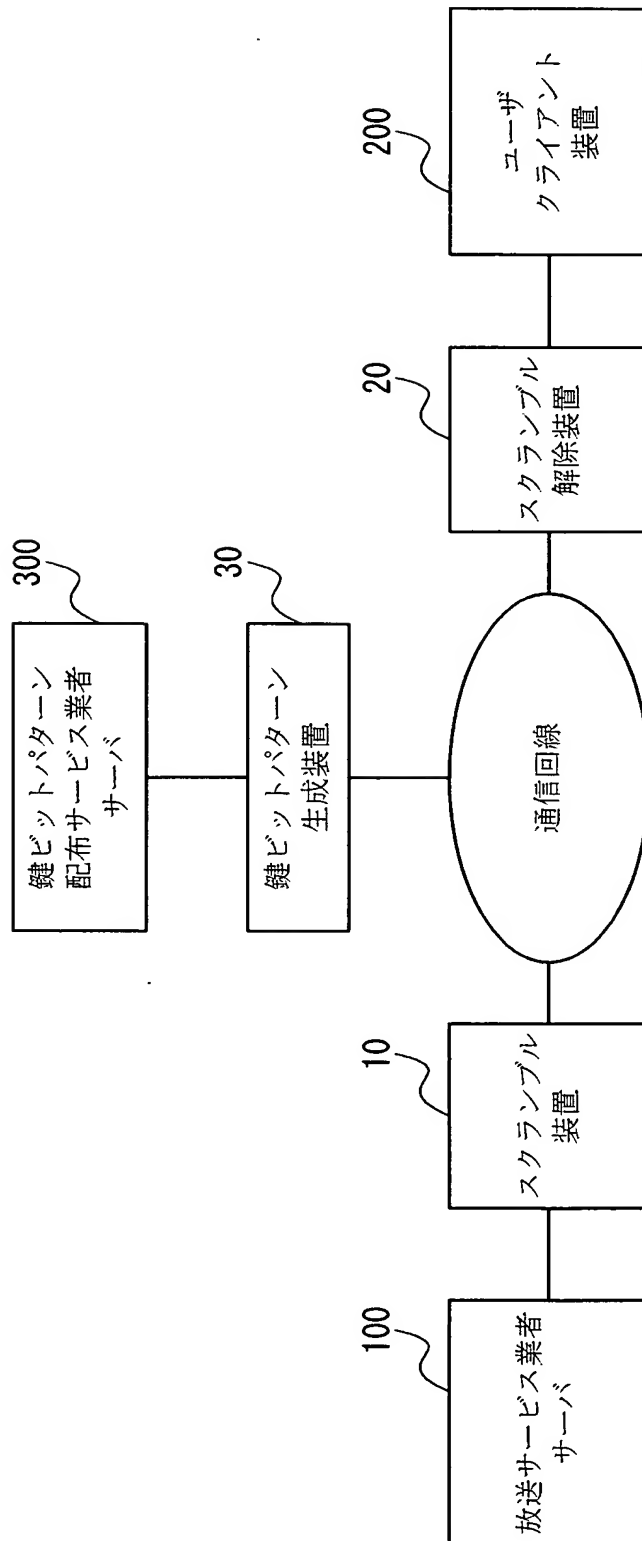
- 1 0 スクランブル装置
- 1 1 鍵ビットパターン管理部
- 1 2 ストリーム符号化部
- 2 0 スクランブル解除装置
- 2 1 鍵ビットパターン管理部
- 2 2 ストリーム復号化部
- 3 0 鍵ビットパターン生成装置
- 4 0 生ストリームメディアデータ
- 5 0 鍵ビットパターン
- 6 1 スクランブルストリームデータ
- 8 0 鍵ビットパターン
- 9 1 生ストリームメディアデータ

【書類名】 図面

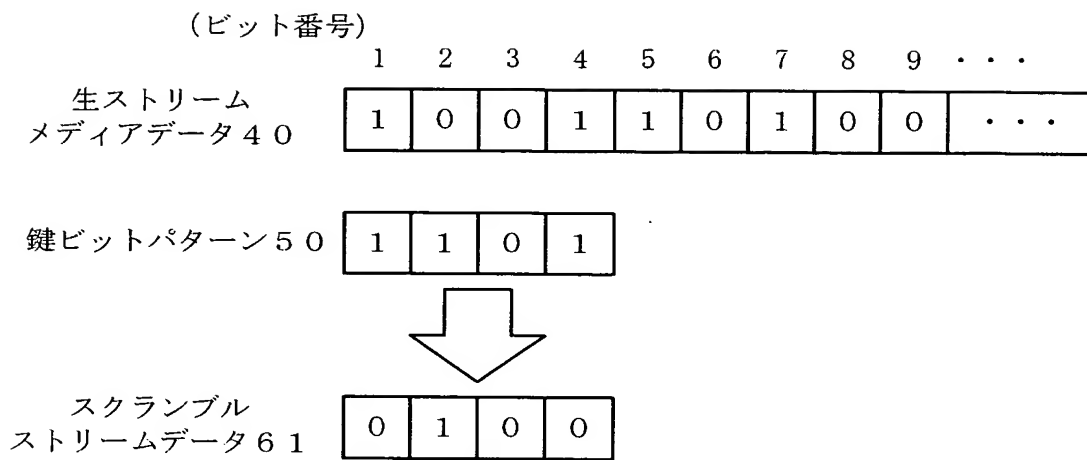
【図 1】



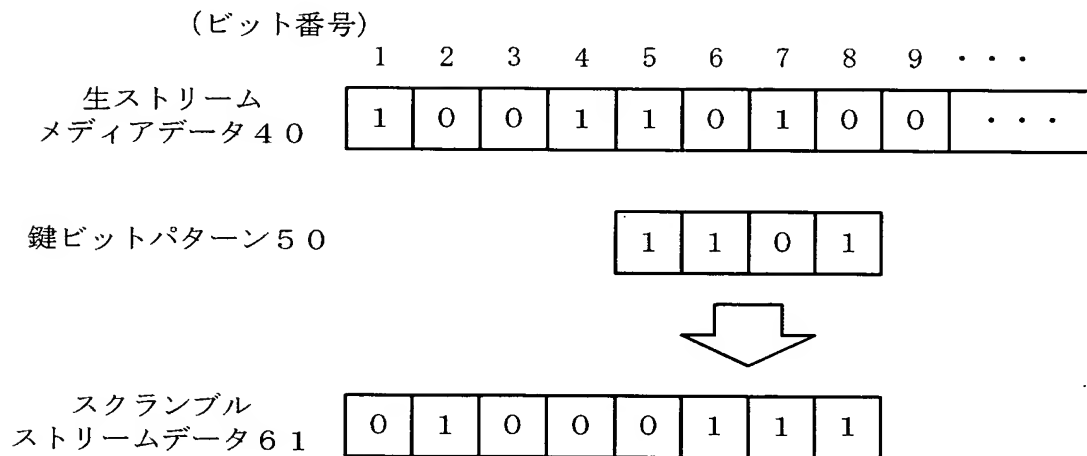
【図 2】



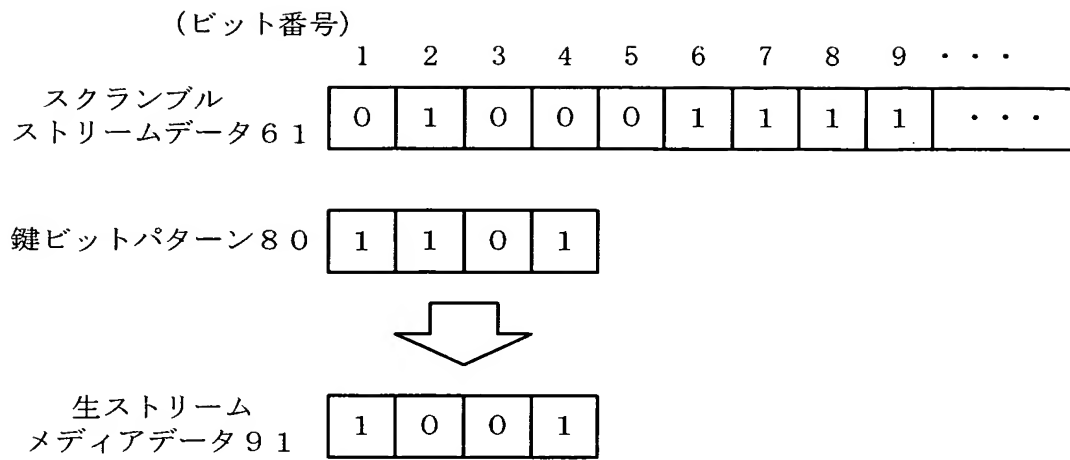
【図 3】



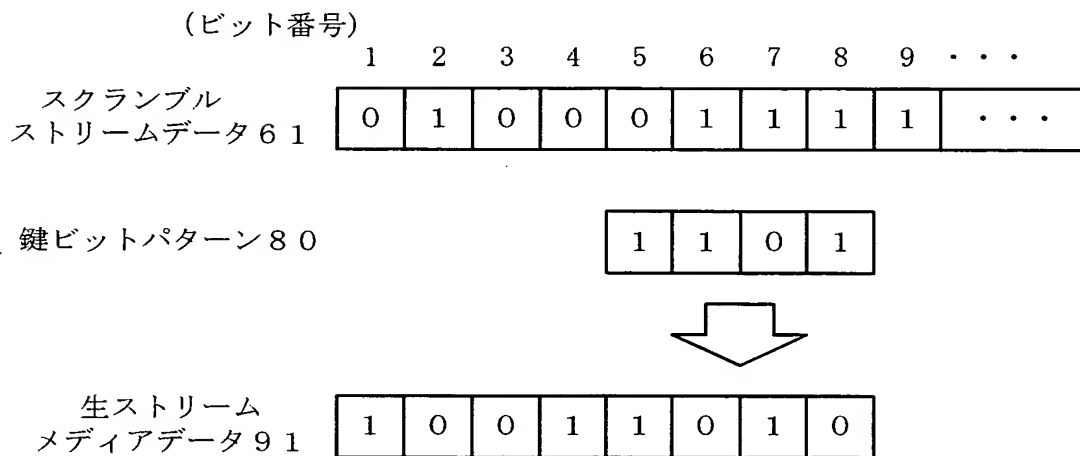
【図 4】



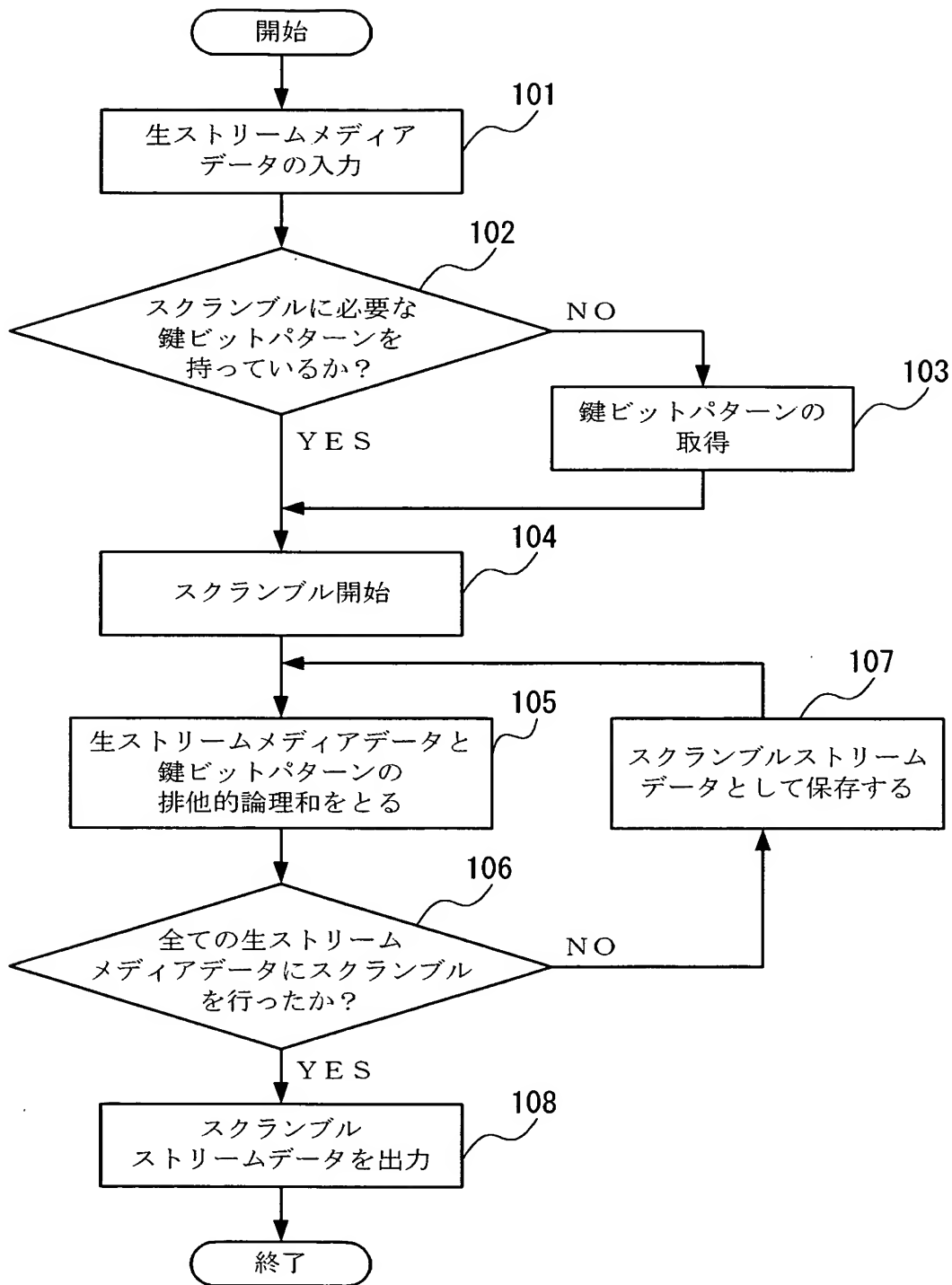
【図 5】



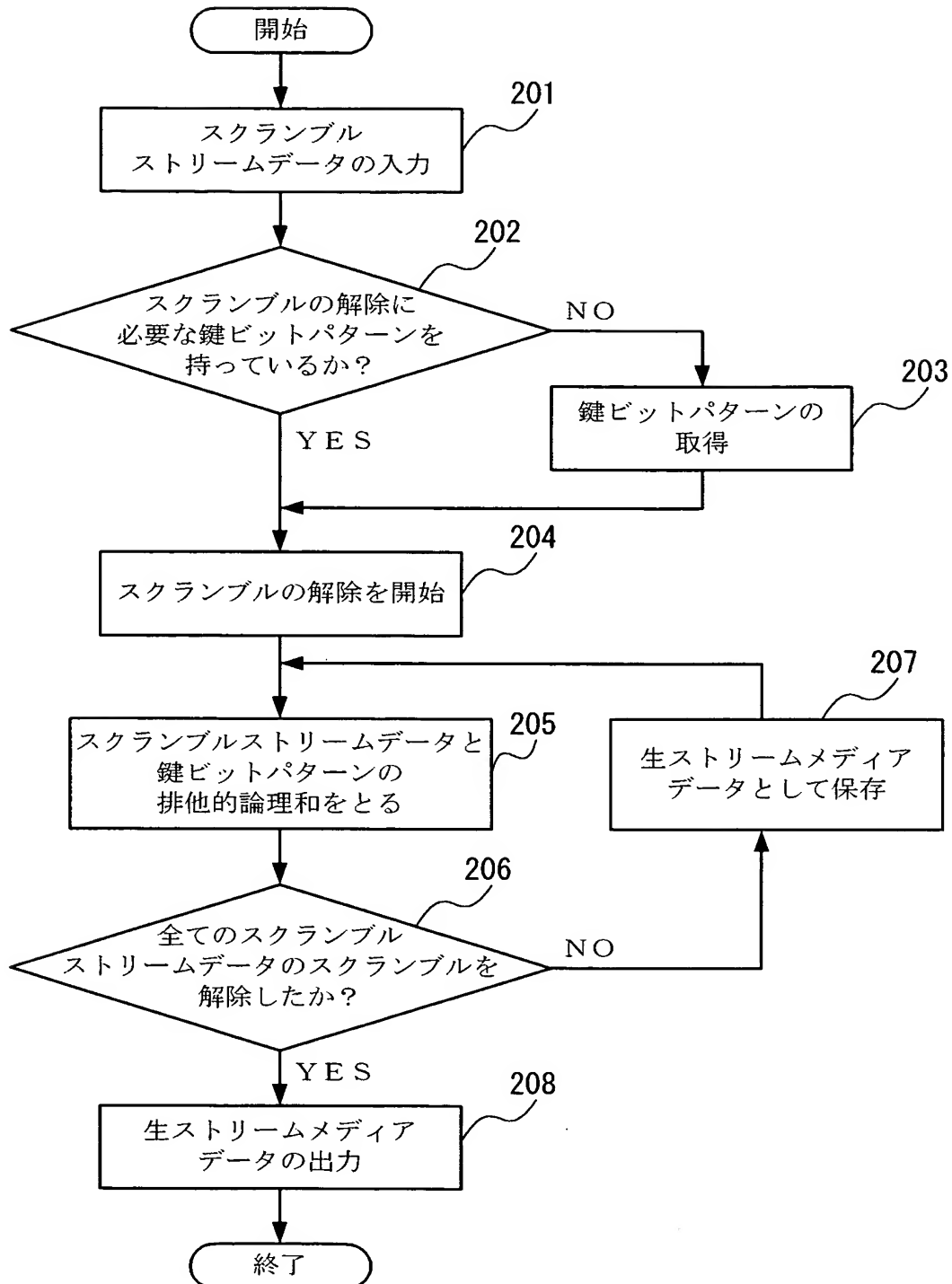
【図 6】



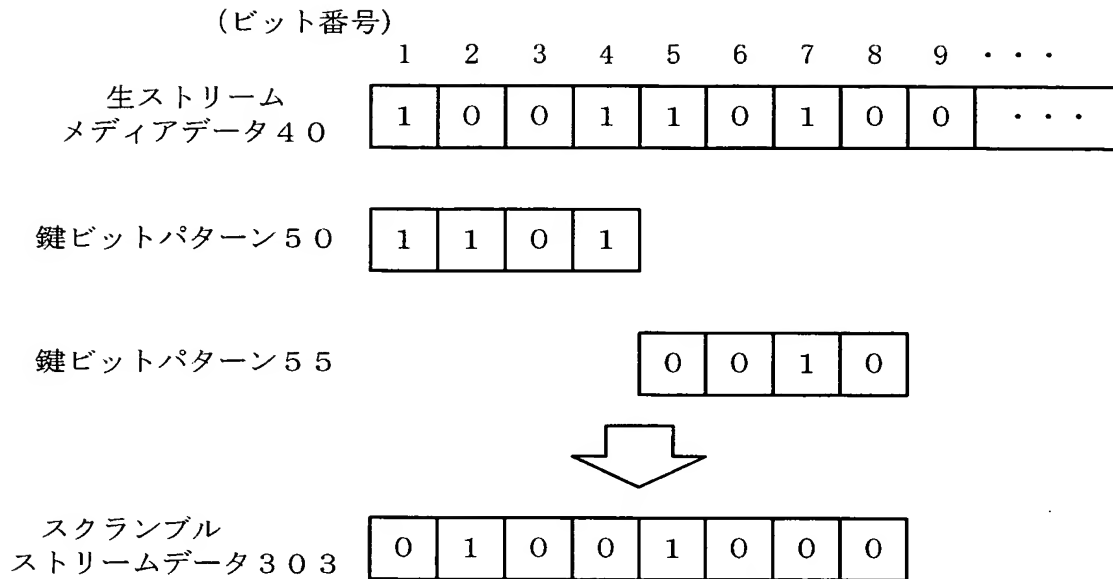
【図 7】



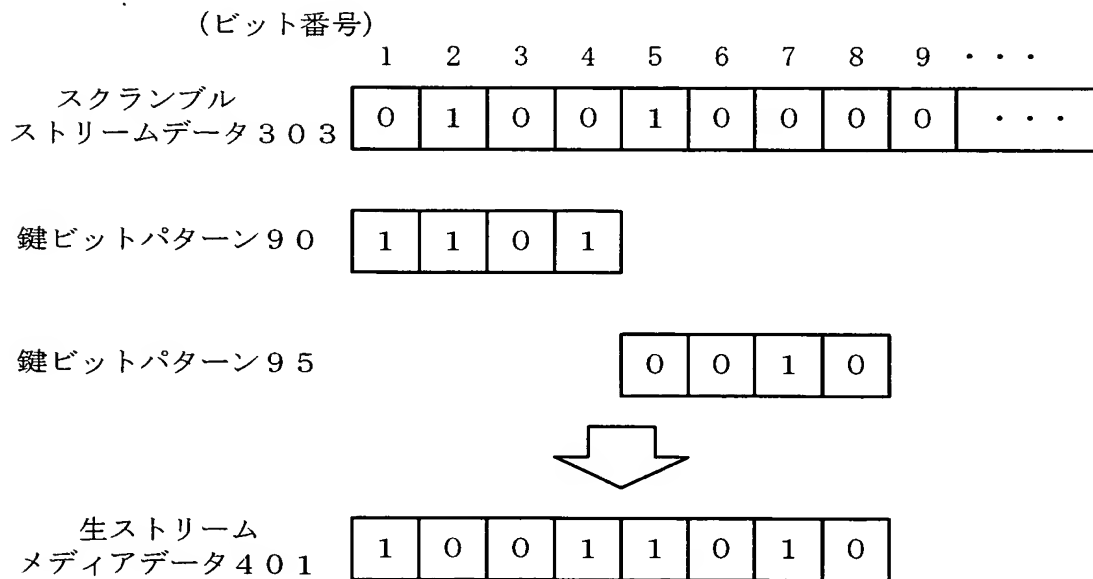
【図 8】



【図 9】



【図 10】



【書類名】 要約書**【要約】**

【課題】 ストリームメディアデータに対して高速な符号化と復号化を施し、スクランブル放送を符号化及び復号化のための専用ハードウェアなどを特に必要とせず簡単に行なうことを可能にする。

【解決手段】 配信側がストリームメディアデータを暗号鍵によって符号化して通信回線を介して配信し、受信側が配信されたストリームメディアデータを暗号鍵によって復号化するストリームメディアデータのスクランブル放送システムは、前記暗号鍵としての所定ビット数の鍵ビットパターンを生成する鍵ビットパターン生成装置 3 0 を備え、前記配信側は、所定の時間的間隔で、鍵ビットパターン生成装置から生成される異なる鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行い、受信側は、配信側と同じ鍵ビットパターンを用いて前記ストリームメディアデータの復号化を行う。

【選択図】 図 1

認定・付加情報

特許出願の番号	特願 2 0 0 2 - 3 3 5 4 0 1
受付番号	5 0 2 0 1 7 4 6 5 3 3
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 4 年 1 1 月 2 0 日

< 認定情報・付加情報 >

【提出日】	平成14年11月19日
-------	-------------

次頁無

特願 2 0 0 2 - 3 3 5 4 0 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 4 2 3 7]

1. 変更年月日

1 9 9 0 年 8 月 2 9 日

[変更理由]

新規登録

住 所

東京都港区芝五丁目 7 番 1 号

氏 名

日本電気株式会社

特願 2 0 0 2 - 3 3 5 4 0 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 2 3 2 2 5 4]

1 . 変更年月日

1 9 9 0 年 8 月 3 0 日

[変更理由]

新規登録

住 所

東京都港区三田 1 丁目 4 番 2 8 号

氏 名

日本電気通信システム株式会社